UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/489,696	01/24/2000	Shigeo Tsujii	FORM PTO-1082	6150

26021 7590 12/01/2005

HOGAN & HARTSON L.L.P.
500 S. GRAND AVENUE
SUITE 1900
LOS ANGELES, CA 90071-2611

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 12/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/489,696	TSUJII ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/08/2005 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-9 and 13-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *3-6,8,13-21 and 23* is/are allowed.

6)☒ Claim(s) *7,9 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on September 08, 2005 has been entered. Claims 3-9 and 13-23 are pending. Claims 1-2 and 10-12 are canceled by applicant. Claims 9 and 21-23 are amended.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 7, 9 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baba (US 5,987, 129), further in view of Matyas (US 4,736,423).

a. *Referring to claim 7:*

i. Baba teaches:

(1) storage means at each entity for storing secret keys peculiar to each respective entity produced for respective pieces of information resulting from division of information specifying each of said respective entities, the divided information used to generate the secret keys allowing diminished sizes of the secret keys; **[i.e., referring to Figure 1, When each entity 2 receives the secret private key Xn and the identifier transformation algorithm, it stores them secretly in a suitable storage device of its own computer (column 10, lines 14-16)];**

(2) selection means for selecting components corresponding to pieces of information specifying opposite entities to be communicated with, from among the secret keys stored; and means for generating said common keys using said components so selected **[i.e., in the cryptosystem, the secret private key of each entity 2 is generated and a common cryptokey is generated according to a linear transformation or scheme. It is assumed that Xif represents the secret private key of an entity i for the generation of a common cryptokey shared by f entities 2. According to a general concept for constructing the above linear**

scheme, that is "selection", an f-input symmetric transformation g (which is a symmetric function having f variables) is arbitrarily selected (column 15, lines 12-20)].

ii. Though Baba teaches the claimed subject matter, Baba does not explicitly mention the generator which generates the secret keys (column 9, lines 7-20 and column 10, lines 52-65) could reduce the sizes of the secret keys. On the other hand, Matyas teaches:

(1) A technique is provide in Matyas' invention for reducing RSA crypto variable storage from 1200 bits (400-bit public key, 400-bit secret key, and 400-bit modulus) to 10 bits. Of the 106 bits, only 56 bits (denoted X) must be kept secret. The size of X has thus been chosen to maintain equivalence with the DES **(column 3, lines 65-68 through column 4, lines 1-3 of Matyas).** Furthermore, Matyas' invention shows a method that allows the public key and modulus (amounting to 800 bits) to be regenerated from only 260 bits of public information. Thus, by decrypting these 260 bits, no more than 400 bits of data will be produced that requires transmission. This is the minimum that must be transmitted and represents the best that could be done under any conditions. However, since 260 bits must be padded with roughly 140 bits to form a full block before decryption with the secret key and public modulus of the key distribution center can be performed, there are, in effect, 140 extra bits available that can be used very effectively to enhance the security of the distribution protocol at no extra penalty in terms of the number of transmitted bits. For example, these bits could include 56 redundant zero bits to allow the block of recovered data to be properly authenticated, a time-variant parameter or sequence number to allow the receiver to test that the crypto variable is not stale and is received in proper sequence, and an ID of the user to whom the public key and modulus belongs to insure that the crypto variables belong to the user for whom the request is being made **(column 6, lines 53-68 through column 7, lines 1-6 of Matyas).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matyas into Baba's invention to encryption techniques for code stored on magnetic stripe cards and, more particularly, to techniques for reducing RSA (Rivest, Shamir, and Adleman algorithm) crypto variable storage size so that the RSA algorithm is compatible with magnetic stripe cards **(column 1, lines 9-14 of Matyas).**

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matyas into Baba's invention since in order for the RSA algorithm to be workable in banking applications, either a new magnetic stripe card with more storage must be developed or a more efficient way to store the secret key and modulus on the present magnetic stripe card must be found. Being incompatible with present magnetic stripe cards is a major disadvantage that would most likely impede the acceptance of public key algorithms. Applications involving personal keys (an especially important feature of public key cryptography) will thus be negatively impacted unless efficient techniques for storing parameters on the magnetic stripe card can be found or present card storage capabilities are extended. **(column 3, lines 40-52 of Matyas).**

b. *Referring to claim 9:*

i. Baba teaches:

(1) a computer readable recording medium that stores a program that generates at entities involved in communications common keys used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext to said plaintext in a cryptographic communications system, comprising: first program code means for causing said computer to select a component corresponding to one or more of divided pieces of information specifying one entity from a secret key peculiar to another entity, the divided information allowing diminished sizes of the secret keys; and second program code means for causing said computer to generate said common keys using said components selected **[i.e., as shown in Figure 8, the computer of each of the entities 2 comprises a keyboard 4, a main unit 5 made up of a CPU, a RAM, a ROM, etc., and a data base 6 comprising a hard disk, that is "a computer readable recording medium", or the like for storing the secret private key xn, the identifier**

transformation algorithm, plaintexts such as sentences, programs (which can include "first program code and second program code"), etc., and encrypted communication texts (column 12, lines 19-25)].

ii. Though Baba teaches the claimed subject matter, Baba does not explicitly mention the generator which generates the secret keys (column 9, lines 7-20 and column 10, lines 52-65) could reduce the sizes of the secret keys. On the other hand, Matyas teaches:

(1) A technique is provide in Matyas' invention for reducing RSA crypto variable storage from 1200 bits (400-bit public key, 400-bit secret key, and 400-bit modulus) to 10 bits. Of the 106 bits, only 56 bits (denoted X) must be kept secret. The size of X has thus been chosen to maintain equivalence with the DES **(column 3, lines 65-68 through column 4, lines 1-3 of Matyas).** Furthermore, Matyas' invention shows a method that allows the public key and modulus (amounting to 800 bits) to be regenerated from only 260 bits of public information. Thus, by decrypting these 260 bits, no more than 400 bits of data will be produced that requires transmission. This is the minimum that must be transmitted and represents the best that could be done under any conditions. However, since 260 bits must be padded with roughly 140 bits to form a full block before decryption with the secret key and public modulus of the key distribution center can be performed, there are, in effect, 140 extra bits available that can be used very effectively to enhance the security of the distribution protocol at no extra penalty in terms of the number of transmitted bits. For example, these bits could include 56 redundant zero bits to allow the block of recovered data to be properly authenticated, a time-variant parameter or sequence number to allow the receiver to test that the crypto variable is not stale and is received in proper sequence, and an ID of the user to whom the public key and modulus belongs to insure that the crypto variables belong to the user for whom the request is being made **(column 6, lines 53-68 through column 7, lines 1-6 of Matyas).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matyas into Baba's invention to encryption techniques for code stored on magnetic stripe cards and, more particularly, to techniques for reducing RSA (Rivest, Shamir, and Adleman algorithm) crypto variable storage size so that the RSA algorithm is compatible with magnetic stripe cards **(column 1, lines 9-14 of Matyas).**

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matyas into Baba's invention since in order for the RSA algorithm to be workable in banking applications, either a new magnetic stripe card with more storage must be developed or a more efficient way to store the secret key and modulus on the present magnetic stripe card must be found. Being incompatible with present magnetic stripe cards is a major disadvantage that would most likely impede the acceptance of public key algorithms. Applications involving personal keys (an especially important feature of public key cryptography) will thus be negatively impacted unless efficient techniques for storing parameters on the magnetic stripe card can be found or present card storage capabilities are extended. **(column 3, lines 40-52 of Matyas).**

g. *Referring to claim 22:*

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

Response to Argument

4. Applicant's arguments filed September 08, 2005 have been fully considered but they are not persuasive.

Applicant argues that:

"Independent 9 and 22 require secret keys peculiar to each respective entity produced for respective pieces of information resulting from division of information specifying each of said respective entities, which is neither disclosed nor fairly suggested by Baba."

Examiner still maintains that:

Baba does teach the claimed subject matter. In addition, referring to Figure 3, generating, in the center, that could be a plurality of centers (see column16,

line 8) , **a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities** and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities (column 2, lines 50-57 of Baba). Baba further teaches a center or central facility established on the network generates a secret private key for each of the entities for generating a common cryptokey and distributes the generated secret private key to each of the entities. When the entities communicate with each other, each of the entities applies its own secret private key to the other entity's identifier (name, address, or the like), generating a common cryptokey shared by the entities (column 1, line 40 through column 2, line 5 of Baba). Furthermore, since the center matrix c is a symmetric matrix, the common cryptokeys Kij, Kji are obviously equal to each other (Kij=Kji). Therefore, the common cryptokeys Kij, Kji which are separately generated by the respective entities i, j coincide with each other, so that the entities i, j can share the common cryptokey (column 11, lines 17-22 of Baba). Whereas, Matyas teaches a **technique for reducing RSA (Rivest, Shamir and Adleman algorithm) cryptovariable key** from 1200 bits (400-bit public key, 400-bit secret key and 400-bit modulus) to 106 bits makes feasible the storage of the RSA algorithm parameters on current magnetic stripe cards used by the banking and finance industry. Of the 106 bits required, only 56 bits must be kept secret; the remaining 50 bits are nonsecret. These 106 bits are used to derive two 200-bit primes P and Q from which is computed the modulus N=PQ and two 400-bit keys PK (public key) and SK (secret key). In effect, a savings in storage is achieved at the expense of performing a precomputation to derive the modulus and keys each time the system is utilized for encryption/decryption (see Matyas' abstract). Besides, Baba and Matyas do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably

distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of Baba and Matyas is sufficient.

For the above reasons, it is believed that the rejections for claims 7, 9, and 22 should be sustained.

Allowable Subject Matter

5. Claims 3-6, 8, 13-21, and 23 are allowed.

Conclusion

6. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Primary Examiner
Art Unit 2135

TBT
November 23, 2005